REMARKS

Claims 1, 37, and 38 have been amended to clarify the subject matter regarded as the invention. Claims 1-18 and 29-38 are pending.

The Examiner has rejected claims 1-6, 18, 37 and 38 under 35 USC 102(e) as being anticipated by Schultz and claims 7, 8, 10, 12-17, and 29-34 under 35 USC 103(a) as being unpatentable over Schultz in view of Tajalli.

The rejection is respectfully traversed. With respect to claims 1, 37, and 38, each recites updating a first risk level determined by static analysis of an executable to a second risk level "if a process started by the executable after the executable has been allowed to execute is observed to perform or attempt an action with which the second risk level is associated." Schultz describes detecting malicious executables by analyzing byte sequences extracted from the binary code of such executables and applying a set of detection rules designed to detect sequences associated with malicious code. Schultz paragraphs [0104] – [0106] and [0109]. Schultz describes updating the rule set periodically, based on offline analysis by experts of executables classified originally as "borderline", i.e., a definitive determination could not be made using the existing rules as to whether or not the executable was malicious. Schulz paragraphs [0107] and [0108]. The analysis describe by Schultz is performed statically on binary code comprising the executable, prior to the executable being allowed to execute on a system to which it has been sent. Purely static analysis (i.e., not while the executable is executing), with periodic offline refinement of a set of rules used to perform the static analysis, is not the same as allowing an executable assigned a first risk level to execute and then updating the first risk level to a second risk level ""if a process started by the executable after the executable has been allowed to execute is observed to perform or attempt an action with which the second risk level is associated," as recited in claims 1, 37, and 38. As such, claims 1, 37, and 38 appear to be allowable.

Claims 2-18 and 29-36 depend from claim 1 and are believed to be allowable for the same reasons described above.

The foregoing amendments are not to be taken as an admission of unpatentability of any of the claims prior to the amendments.

Reconsideration of the application and allowance of all claims are respectfully requested based on the preceding remarks. If at any time the Examiner believes that an interview would be helpful, please contact the undersigned.

Respectfully submitted,

Dated: 11/30/07

William J. James
Registration No. 40,661
V 408-973-2592
F 408-973-2595

VAN PELT, YI & JAMES LLP
10050 N. Foothill Blvd., Suite 200
Cupertino, CA 95014